UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/670,298	09/26/2003	Andrea Klaes	SRE-0003-US	6494

36183 7590 05/30/2008

PAUL, HASTINGS, JANOFSKY & WALKER LLP
875 15th Street, NW
Washington, DC 20005

EXAMINER	
SHAN, APRIL YING	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/670,298	KLAES, ANDREA	
	Examiner	Art Unit	
	APRIL Y. SHAN	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 May 2007* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 3/13/2008, PROSECUTION IS HEREBY REOPENED. The 103 rejection based on Khanolkar et al. is withdrawn. However, after careful search, new ground of rejections are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

2. Claims 1-30 have been examined.

3. Any rejection/objection not repeated below for record are withdrawn.

Response to Argument

4. The Applicant's remark/argument in view of Khanolkar in the Appeal brief is summarized as below: Some of them are persuasive and some are not.

a. The Applicant argues: "the central loghost and proxy loghost are separated by the network. Thus, the central loghost and the proxy loghost are remote from each other. Khanolkar does not suggest this remote configuration", the examiner respectfully points out on page 8 of the Appeal brief, the Applicant stated "As those of ordinary skill in the computer related arts appreciate...the word remote may simply mean that two or more elements, entities, or elements are **spatially separate, but a great amount of separation is not required**". In the fig. 2 of the Khanolkar reference, event parser 54 and event manager 55 are separate entities and therefore, they are remote according to Applicant. Please also note "separated by the network" is not in the claims. The claims recited "…proxy loghost remote from the central loghost and in communication with the central loghost over a network" instead. However, Khanolkar reference does not expressly disclose event parser 54 and event manager 55 are communication over a network, but to a person with ordinary skill in the art, separate entities within the same system are connected by the local area network (LAN). In the below new grounds of rejections, both Khanolkar in view of Esbensen and Ko in view of Khanolkar references teach the feature of proxy loghost remote from the central loghost and in communication with the central loghost over a network (Please see below).

b. The Applicant argues: "Claim 12 recites that the central loghost receives and analyzes log files and events. Khanolkar fails to suggest a central loghost that

receives log files and events, and instead only discloses the event manager 55 as receiving event objects, not log files as claimed", the examiner respectfully agrees. Please see below new ground rejections that both Khanolkar in view of Esbensen and Ko in view of Khanolkar teach the feature of the central loghost receives and analyzes log files and events.

c. The Applicant argues: "claim 9 Khanolar suggests ...storing only event objects..", the examiner found this argument persuasive. Please see below new ground rejection Knanolkar in view of Esbensen disclose the archiving of log files on the proxy loghost and the archiving of events on the central loghost.

Drawings

5. Figure 1 is objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "150" and "160" have been used to designate different networks and different proxy loghosts. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claim 1**, “at least one proxy loghost…in communication with the central loghost over a network” and "wherein the proxy loghost receives...on the network..." are being recited. However, in the replacement fig. 1 of the original disclosure (Filed on 16 May 2007), it appears to the examiner although each network marked as "150", they are indeed different networks. Please look closely at the figure 1 that all loghosts (both central and proxy) is in communication with the center network 150 via firewalls. It is well known in the art behind each firewall, there is a respectively local area network/Wide area network. Please also see in par. [0022] of the original disclosure, the Applicant discloses “In accordance with the embodiments of the present invention, log files, and that maybe in communication with **a respective network 150**…”. Therefore, it is incorrect that each network recited in claim 1 is same network as claimed by the Applicant. In order to further examine the merits of the claims, the examiner assumes the center network 150 as wide area network (i.e. internet), which can include communication channels to couple together local networks, a central loghost and proxy loghosts.

As per **claim 12**, “a secure network" and "over a network" are being recited. It is not clear whether they are same network or different respective network. Please note in the replacement figure 1 that all loghosts (both central and proxy) is in communication with the center network 150 via firewalls. It is well known in the art behind each firewall, there is a respectively local area network/Wide area network. Please also see in par. [0022] of the original disclosure, the Applicant discloses “In accordance with the embodiments of the present invention, log files, and that maybe in communication with **a respective network 150**…”. In order to further examine the merits of the claims, the examiner assumes the center network 150 as wide area network (i.e. internet), which can include communication channels to couple together local networks, a central loghost and proxy loghosts.

As per **claim 22**, “…over a network from the proxy loghost…” and “…alarm…an unwanted incident in the network” are being recited. However, in the replacement fig. 1 of the original disclosure (Filed on 16 May 2007), it appears to the examiner although each network marked as "150", they are indeed different networks. Please look closely at the figure 1 that all loghosts (both central and proxy) is in communication with the center network 150 via firewalls. It is well known in the art behind each firewall, there is a respectively local area network/Wide area network. Please also see in par. [0022] of the original disclosure, the Applicant discloses “In accordance with the embodiments of the present invention, log files, and that maybe in communication with **a respective network 150**…”. It is not clear whether "alarm...of an unwanted incident in the network"

is the same network as "over a network" recited in the same claim or any other respective network as in fig. 1. In order to further examine the merits of the claims, the examiner assumes the center network 150 as wide area network (i.e. internet), which can include communication channels to couple together local networks, a central loghost and proxy loghosts.

Any claim not specifically rejected above is rejected based on a claim which it depends on.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 1-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

In claims 1-21, a “computer-implemented system” is being recited; however, it appears that the system would reasonably be interpreted by one of ordinary skill in the art as software, per se. On page 5, par. [0017] of the specification, the Applicant defined “both proxy and central loghosts are **independent modules**…” and on page 6, par. [0019] of the specification, the Applicant discloses “…several **software modules that comprise central loghost and proxy loghost**…the basic operating system is based on a Solaris Operating System…Unix-styled systems such as Linux...”. Please

note to a person with ordinary skill in the art, in Unix/Linux, a module is **a collection of routines** (software only) that perform a system-level function, and maybe dynamically loaded and unloaded as required. Further, in par. [0020] of the original disclosure, the Applicant discloses "A **secure shell daemon (sshd)** operates to exchange data between proxy loghost and central loghost". To a person with ordinary skill in the art, in Unix, sshd is a computer program that runs in the background to handle incoming secure shell connections over the network. The secure shell daemon is the computer program securely communicates data between proxy loghost and central loghost over the network (i.e. internet) and secure shell daemon is software. Also, on page 4, par. [0015] of the specification, the Applicant defined "resources" is to be constructed broadly as "any system that may be connected to (or operating within) a given network and that generates log files….many enterprise software applications…and the like generate log files….". All other claim limitations such as software adapters, module, log files are software. As such, it believes that the system of claims 1-21 are reasonably interpreted as functional descriptive material, per se. "Functional descriptive material consists of data structures and computer programs which impart functionality when employed as a computer component." (MPEP 2106). Also, the Applicant is respectfully reminded a preamble (computer-implemented) is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand

alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

12. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

13. Claims 1-7, 9-17, 19-28 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar et al. (U.S. Patent No. 7,127,743) in view of Esbensen (U.S. Patent No. 5,796,942).

As per **claim 1**, Khanolkar et al. discloses a computer-implemented monitoring/intrusion system/method, comprising:

a central loghost (event manager 55 in fig. 2 corresponds to Applicant's event manager),

at least one proxy loghost (event parser 54 in fig. 2 corresponds to Applicant's proxy loghost), remote from the central loghost (Please see in fig. 2, event manager 55 and event parsers 54 are two separate entities. Please also note in the Appellant's appeal brief lines 21-25 of page 8, Appellant stated "As those of ordinary skill in the computer related arts appreciate, the word "remote" does not necessarily describe or denote great distance between a plurality of elements. To the contrary, the word remote may simply mean that two or more elements, entities, or elements are spatially separate...". Thus, event manager 55 and event parsers 54 are remote from each other according to Appellant's above statement. **Also, the secondary reference Esbensen discloses the feature of central loghost and proxy loghost are remote from each other. Please follow the rejection in view of Esbensen**) and

at least one monitoring station (event broadcaster 56 in fig. 2 corresponds to Applicant's monitoring station),

wherein the proxy loghost receives a plurality of log files from a plurality of resources operating on the network, analyzes the log files for at least one of unexpected volume, unexpected patterns, or unexpected types of log files, and generates events in view of such analysis ("an event parser in communication with multiple network service devices, wherein the network service devices comprise a firewall, VPN (virtual private network) server or router, an e-mail server, or any combination of two or more thereof, the event parser being able to receive log data in real time from the device, the log data including information detailing a network intrusion event received from the network service device if an intrusion has occurred, the event parser being able to parse the information to create corresponding event objects concerning the intrusion events, wherein an event object comprises information fields relevant to network security monitoring including at least information regarding a reporting device and a time stamp" – e.g. claim 1),

wherein the central loghost is operable to receive the events generated by the proxy loghost and generate an alert upon an analysis of the events, and wherein the monitoring station is caused to issue an alarm when the alert is generated ("an event manager in communication with the event parser, the event manager being able to receive the event objects, the event manager being configured to evaluate the event objects according to at least one predetermined threshold condition such that, when the event objects satisfy the predetermined threshold condition, the event manager

designates the event objects to be broadcast in real time an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast, the event broadcaster being able to transmit the event objects in real time, relative to the receipt of the log
data, as an intrusion alarm…" – e.g. claim 1).

Khanolkar et al. does not expressly disclose a central loghost and the plurality of proxy loghosts are in communication over a network.

However, Esbensen discloses a central loghost and the plurality of proxy loghosts are in communication over a network ("Remote Surveillance Agent, FIGS. 4 and 5 illustrate a different embodiment of the invention wherein a number of remote surveillance agents (RSAs) may be utilized along with an internet in order to capture network data traffic on one site and have that traffic analyzed and sessions reconstructed at another site. FIG. 4 shows RSAs 100a-c connected to different WAN/LAN networks 105a. According to this embodiment, RSAs 100a-c collect all network data traffic from the LAN or WAN to which they are attached, but instead of fully scanning that traffic, RSAs 100a-c store collected packets into a form that may be transmitted to remote surveillance server (RSS) 110. RSS 110 receives the information for RSAs 100a-c and presents this information to a surveillance system 1 according to the invention, which performs session reconstruction, rule checking, and alert handling as described above. According to one specific embodiment RSAs 100a-c collect multiple packets on their attached WAN/LAN and compress multiple packets

into a single internet packet which may be transmitted back through the WAN/LAN, over the internet, to RSS 110. According to this embodiment, RSAs 100a-c can in this way allow a surveillance system 1 located in one city to monitor several WAN/LANs located in different cities simply by plugging an RSA into the remote network without making any other changes to the network..." – e.g. col. 7, lines 19-54, fig. 4 and fig. 5. Please note Remote Surveillance Agent (RSA) corresponds to Applicant's proxy loghosts and RSS 110 AND Survellance System correspond to Applicant's central loghost. From this passage and the figures, RSA and RSS-Survellance Systems are **remote** from each other and in communication over internet. Please note internet is the worldwide, publicly accessible network).

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate Esbensen's a central loghost and the plurality of proxy loghosts are in communication over a network and the log files also are received by the central loghosts into Khanolkar et al. 's system motivated by to allow central loghost located in one location to monitor serveral WAN/LANs located in different location simply by plugging proxy loghosts into the remote network without making any other changes to the network (Esbensen, col. 7, lines 40-43).

As per **claim 2**, Khanolkar et al. - Esbensen discloses a system as applied in claim 1. Khanolkar et al. further discloses wherein the central loghost comprises a plurality modules operating in a Unix environment ("system 10 is preferably…implemented on …Linux or Solaris server platforms…" –e.g. col. 4, lines

11-12). Please note Linux is unix-like operating system and has unix background. Therefore, it met the limitation of the claim.

As per **claim 3**, Khanolkar et al. – Esbensen discloses a system as applied in claim 1. Khanolkar et al. further discloses comprising a plurality of proxy loghosts, each one of the plurality being in communication with the central loghost ("an event manager in communication with the event parser" – e.g. abstract and "a plurality of event parsers" – e.g. col. 7, lines 46—54).

As per **claim 4**, Khanolkar et al. – Esbensen discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer (e.g. col. 3, lines 59 – col. 4, line 1).

As per **claim 5**, Khanolkar et al. – Esbensen discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein a plurality of events is required to cause the generation of an alert ("It is also contemplated that a user may set no threshold…and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3)

As per **claim 6**, Khanolkar et al. – Esbensen discloses the system as applied in claim 1. Khanolkar et al. met the limitation of claim 6 by further disclose wherein

security management has access to both the proxy loghost and the central loghost ("….In event manager 55, as well as in other system modules and features, filter settings may be set by a user, for instance, a network administrator through web client interface 30…Settings may be modified by a user during system 10 operation by further input into web client interface 30" – e.g. col. 6, lines 38-54)

As per **claim 7**, Khanolkar et al. - Esbensen discloses the system as applied in claim 1. Khanolkar et al. further discloses wherein the log files are received from a network-based intrusion detection system (e.g. col. 2, lines 1-9)

As per **claim 10**, Khanolkar et al. – Esbensen discloses the system as applied in claim 1. Khanolkar et al. further discloses comprising software adapters to convert one format of a log file to another format ("…log data…are converted to event objects for processing and manipulation by the system…" –e.g. col. 2, lines 25-32).

As per **claim 11**, Khanolkar et al. – Esbensen discloses the system as applied in claim 1. Khanolkar et al. further discloses comprising a module for visualizing the log files received at the proxy loghost ("system 10 operates in conjunction with a web server, such as Apache or Netscape" – e.g. col. 4, lines 14-15).

As per **claims 12 and 22**, Khanolkar et al. discloses a computer-implemented monitoring/intrusion system/method, comprising:

a plurality of proxy loghosts, each proxy loghost collecting log files that are generated by resources in a portion of the secure network, the plurality of loghosts generating events in response to the log files collected ("an event parser in communication with multiple network service devices, wherein the network service devices comprise a firewall, VPN (virtual private network) server or router, an e-mail server, or any combination of two or more thereof, the event parser being able to receive log data in real time from the device, the log data including information detailing a network intrusion event received from the network service device if an intrusion has occurred, the event parser being able to parse the nformation to create corresponding event objects concerning the intrusion events, wherein an event object comprises information fields relevant to network security monitoring including at least information regarding a reporting device and a time stamp" – e.g. claim 1 and event parsers 54 in fig. 2. Please note event parsers 54 corresponds to Applicant's proxy loghosts); and a central loghost ("event manager 55" in fig. 2 corresponds to Applicnat's central loghost) remote from the plurality of proxy loghosts (Please see in fig. 2, event manager 55 and event parsers 54 are two separate entities. Please also note in the Appellant's appeal brief lines 21-25 of page 8, Appellant stated "As those of ordinary skill in the computer related arts appreciate, the word "remote" does not necessarily describe or denote great distance between a plurality of elements. To the contrary, the word remote may simply mean that two or more elements, entities, or elements are spatially separate...". Thus, event manager 55 and event parsers 54 are remote from each other according to Appellant's above statement. **Also, the**

secondary reference Esbensen discloses the feature of central loghost and proxy loghost are remote from each other. Please follow the rejection in view of Esbensen) the central loghost receiving the events from the plurality of proxy loghosts, the central loghost analyzing the events to determine the necessity of generating an alert and an associated alarm to notify a security manager of a possible intrusion incident ("an event manager in communication with the event parser, the event manager being able to receive the event objects, the event manager being configured to evaluate the event objects according to at least one predetermined threshold condition such that, when the event objects satisfy the predetermined threshold condition, the event manager designates the event objects to be broadcast in real time an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast, the event broadcaster being able to transmit the event objects in real time, relative to the receipt of the log data, as an intrusion alarm…" – e.g. claim 1)

Khanolkar et al. does not expressly disclose a central loghost and the plurality of proxy loghosts are in communication over a network and the log files also are received by the central loghosts and log file is also analyzed on the central loghost.

However, Esbensen discloses a central loghost and the plurality of proxy loghosts are in communication over a network and the log files also are received/analyzed by the central loghosts ("Remote Surveillance Agent, FIGS. 4 and 5 illustrate a different embodiment of the invention wherein a number of remote surveillance agents (RSAs) may be utilized along with an internet in order to capture

network data traffic on one site and have that traffic analyzed and sessions reconstructed at another site. FIG. 4 shows RSAs 100a-c connected to different WAN/LAN networks 105a. According to this embodiment, RSAs 100a-c collect all network data traffic from the LAN or WAN to which they are attached, but instead of fully scanning that traffic, RSAs 100a-c store collected packets into a form that may be transmitted to remote surveillance server (RSS) 110. RSS 110 receives the information for RSAs 100a-c and presents this information to a surveillance system 1 according to the invention, which performs session reconstruction, rule checking, and alert handling as described above. According to one specific embodiment RSAs 100a-c collect multiple packets on their attached WAN/LAN and compress multiple packets into a single internet packet which may be transmitted back through the WAN/LAN, over the internet, to RSS 110. According to this embodiment, RSAs 100a-c can in this way allow a surveillance system 1 located in one city to monitor several WAN/LANs located in different cities simply by plugging an RSA into the remote network without making any other changes to the network..." – e.g. col. 7, lines 19-54, fig. 4 and fig. 5. Please note Remote Surveillance Agent (RSA) corresponds to Applicant's proxy loghosts and RSS 110 AND Survellance System correspond to Applicant's central loghost. From this passage and the figures, RSA and RSS-Survellance Systems are **remote** from each other and in communication over internet. Please note internet is the worldwide, publicly accessible network. Please further note captured network data traffic corresponds to Applicant's log data). Furthermore, Esbensen discloses "RSS 110 receives the information for RSAs 100a-c and presents this information to a

surveillance system 1 according to the invention, which performs session reconstruction, rule checking, and alert handling as described above" – e.g. col. 7, lines 28-34), which meets the claimed limitation of analysis log file on the central loghost.

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate Esbensen's a central loghost and the plurality of proxy loghosts are in communication over a network and the log files also are received/analyzed by the central loghosts into Khanolkar et al. 's system motivated by to allow central loghost located in one location to monitor serveral WAN/LANs located in different location simply by plugging proxy loghosts into the remote network without making any other changes to the network (Esbensen, col. 7, lines 40-43) .

As per **claims 13 and 23**, Khanolkar et al. – Esbensen discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the central loghost comprises a plurality modules operating in a Unix environment ("system 10 is preferably…implemented on …Linux or Solaris server platforms…" –e.g. col. 4, lines 11-12).

As per **claims 14 and 25**, Khanolkar et al. - Esbensen discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the resources comprise at least one of an operating system, application, firewall, router, switch and loadbalancer (e.g. col. 3, lines 59 – col. 4, line 1).

As per **claim 15**, Khanolkar et al. – Esbensen discloses a system as applied in claim 12. Khanolkar et al. further discloses wherein a plurality of events is required to

cause the generation of an alert ("It is also contemplated that a user may set no threshold…and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3).

As per **claims 16 and 27**, Khanolkar et al. - Esbensen discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein security management has access to both the plurality of proxy loghosts and the central loghost ("….In event manager 55, as well as in other system modules and features, filter settings may be set by a user, for instance, a network administrator through web client interface 30…Settings may be modified by a user during system 10 operation by further input into web client interface 30" – e.g. col. 6, lines 38-54)

.

As per **claims 17 and 28**, Khanolkar et al. - Esbensen discloses a system/method as applied in claims 12 and 22. Khanolkar et al. further discloses wherein the log files are received from a network-based intrusion detection system (e.g. col. 2, lines 1-9)

As per **claims 9, 19 and 30**, Khanolkar et al. - Esbensen discloses a system/method as applied in claims 1, 12 and 22. Esbensen further discloses wherein the log files are archived on the plurality of proxy loghosts and events are archived on the central loghost ("RSAs 100a-c store collected packets into a form that may be transmitted to remote surveillance server (RSS) 110. RSS 110 receives the

information for RSAs 100a-c and presents this information to a surveillance system 1 according to the invention, which performs session reconstruction, rule checking, and alert handling as described above" – e.g. col. 7, lines 28-34 and "The reconstructed session is passed through a series of user-defined rules 38...an incident log 39 contains identifying data of the incident such as the name of the alert, description, user login name, location and a snapshot of the session-with an arrow pointing to the pattern that caused the alert to be triggered - e.g. col. 5, lines 8-21. Please note from the above passages, RSA (proxy server) archieves log files and RSS - surveillance system 1 archieves event data (i.e. incident log)

As per **claim 20**, Khanolkar et al. – Esbensen discloses the system as applied in claim 12. Khanolkar et al. further discloses comprising software adapters to convert one format of a log file to another format ("…log data…are converted to event objects for processing and manipulation by the system…" –e.g. col. 2, lines 25-32).

As per **claim 21**, Khanolkar et al. – Esbensen discloses the system as applied in claim 12. Khanolkar et al. further discloses comprising a module for visualizing the log files received at the proxy loghost ("system 10 operates in conjunction with a web server, such as Apache or Netscape" – e.g. col. 4, lines 14-15).

As per **claim 24**, Khanolkar et al. – Esbensen discloses the method as applied in claim 22. Khanolkar et al. further discloses wherein a plurality of proxy loghosts receive log files (col. 7, lines 38-50).

As per **claim 26**, Khanolkar et al. – Esbensen discloses the method as applied in claim 22. Khanolkar et al. further discloses comprising generating the alert only after a plurality events are received ("Therefore, the determination of whether to broadcast the event object as an intrusion alarm is made nearly instantaneously upon receipt of the event object" – e.g. col. 7, lines 14-22 and "It is also contemplated that a user may set no threshold…and allow the generation of alarms and broadcast of all event objects received at 160" – e.g. col. 7, line 60- col. 8, line 3).

14. Claims 8, 18 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Khanolkar et al. (U.S. Patent No. 7,127,743) in view of Esbensen (U.S. Patent No. 5,796,942) as applied to claims 1-7, 9-17, 19-28 and 30 above, and further in view of Admitted prior art disclosed on line 6 of paragraph [0030], on page 9 - line 2 on page 10 of the specification of the current application.

As per **claim 8**, Khanolkar et al. – Esbensen discloses the limitation in claim 1 above and also in col. 1, line 23, Khanolkar discloses "password attacks", which is a type of attack Host-based intrusion system usually detects. By admitting "to the extent..**host-based systems** have already been implemented" in par. [0030] and in par. [0004] of the instant application, "Serveral commercial tools have been made available to combat such attacks…**these tools** generally fall into one of two catergoires…and

host-based systems…". The claim would have been obvious because with "While **these commercial tools may be useful** in some contexts" as admitted by the Applicant in par. [0004], as a person with ordinary skill has good reason to pursue the known options within his or her technical grasp. In turn, because the log files are received from a host-based intrusion detection system as claimed has the properties predicted by the Applicant's admitted prior art, it would have been obvious to receive log files from a host-based intrusion detection system. *See KSR, 82 USPQ2d at 1397.*

As per **claims 18 and 29**, Khanolkar et al. – Esbensen discloses a system/method as applied in claims 12 and 22 and also in col. 1, line 23, Khanolkar discloses "password attacks", which is a type of attack Host-based intrusion system usually detects. By admitting "to the extent..**host-based systems** have already been implemented" in par. [0030] and in par. [0004] of the instant application, "Serveral commercial tools have been made available to combat such attacks…**these tools** generally fall into one of two catergoires…and **host-based systems**…". The claim would have been obvious because with "While **these commercial tools may be useful** in some contexts" as admitted by the Applicant in par. [0004], as a person with ordinary skill has good reason to pursue the known options within his or her technical grasp. In turn, because the log files are received from a host-based intrusion detection system as claimed has the properties predicted by the Applicant's admitted prior art, it would have been obvious to receive log files from a host-based intrusion detection system. *See KSR, 82 USPQ2d at 1397.*

15. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ko et al. (U.S. Patent No. 6,789,202) in view of Khanolkar et al. (U.S. Patent No. 7,127,743).

As per **claim 1**, Ko et al. discloses a computer-implemented monitoring/intrusion system, comprising:

a central loghost ("Global analyzer 104 within console 102" in fig. 1 corresponds to Applicant's central loghost),

at least one proxy loghost remote from the central loghost and in communication with the central loghost over a network ("local analyzers 130-132" in fig. 1 corresponds to Applicant's proxy loghost. Please note local analyzers are remote from the global analyzer and in communication over Wide area network 106); and

wherein the proxy loghost receives a plurality of log files from a plurality of resources operating on the network, analyzes the log files for at least one of unexpected volume, unexpected patterns, or unexpected types of log files ("Local analyzers 130-132 examine this security information, and if necessary, send information specifying a local security condition to global analyzer…Note that local analyzers 130-132 filter the security information…This prevents global analyzer from becoming overwhelmed by security information from sensors" – e.g. col. 6, lines 42-49) and When local sensors 140-145 receive security information, the security information is relayed back to local analyzers 130-132. Local analyzers130-132 filter this information and relay it back to global analyzer 104" - e.g. col. 4, lines 31-34)

wherein the central loghost is operable to receive the events generated by the proxy loghost through the network and generate an alert upon an analysis of the event (steps 316, 318, 320 and 322 in fig. 3), and

Ko et al. does not expressly disclose proxy loghost generate events in view of analysis and information received by the central loghost are events generated by the proxy loghost.

However, the well known features of proxy loghost generate events in view of analysis and information received by the central loghost are events generated by the proxy loghost are disclosed in Khanolkar et al. (“an event parser in communication with multiple network service devices…to create corresponding event objects concerning the intrusion events...an event manager in communication with the event parser, the event manager being able to receive the event objects, the event manager being configured to evaluate the event objects..." - e.g. claim 1 and please note Khanolkar et al. also discloses analyzes the log files for at least one of unexpected volume, unexpected patterns, or unexpected types of log files in claim 1).

It would have been obvious to a person with ordinary skill in the art to incorporate Khanolkar et al.’s proxy loghost generate events in view of analysis and information received by the central loghost are events generated by the proxy loghost into Ko et al.’s system motivated by to filter log data, which contains information related to intrusion events, to provide a more manageable flow of data (e.g. Khanolkar et al. col. 2, lines 15-20) and centralized global analyzer does not become overwhelmed with too much data (e.g. Ko, et al., col. 1, lines 49-52).

Ko et al. – Khanolkar et al. further discloses at least one monitoring station (Ko et al., "sensor 201" in fig. 2 corresponds to Applicant's monitoring station; Khanolkar et al., "event broadcaster 56" in fig. 2 corresponds to one monitoring station), wherein the monitoring station is caused to issue an alarm when the alert is generated ("Sensor 201 is a local intrusion detection component that monitors activity in an assigned portion of networked computer system 100. Sensor 201 can be configured dynamically by analyzer 200 to detect specific security-related events and local intrusions within the assigned portion of networked computer system 100. Sensor 201 can additionally be tuned to quickly react to on-going large-scale intrusions in a manner that is consistent" – e.g. Ko et al., col. 5, lines 39-46 and steps 326-328 in fig. 3; Khanolkar et al., col. 7, lines 14-22 and col. 7, line 53 – col. 8, line 11).

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO -892). Applicant is **strongly urged** to review these references in response to the current office action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2135
/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135